In the Claims

1.-62 (cancelled)

63. (currently amended) A method for providing authenticated access to a controlled network, comprising:

first authenticating a wireless access point to an unauthenticated client device communicatively coupled to the wireless access point via a wireless connection, wherein the first authenticating further comprises:

receiving a first message from said unauthenticated client device at said wireless access point, said first message including a device identifier and a first random number;

receiving a second message from said wireless access point at said unauthenticated client device, said second message including a second random number and a first digest, said first digest including a one-way hash function operating on said first random number, said device identifier, and a first secret shared between said wireless access point and said unauthenticated client device;

determining a second digest at said unauthenticated client device, said second digest comprising a one-way hash function operating on said first random number, said device identifier, and said first secret;

comparing said first digest to said second digest at said unauthenticated client device; and

provided said first digest matches said second digest, authenticating said wireless access point to said unauthenticated client device;

second authenticating the unauthenticated client device to the wireless access point to produce an authenticated client device and a key; <u>and</u>

third authenticating, via the wireless access point, a user of the authenticated client device to a central authentication server using the key.

64. (previously presented) The method of claim 63 wherein the first authenticating and the second authenticating comprise a shared secret key exchange between the wireless access point and the unauthenticated client device.

65. (cancelled)

66. (currently amended) The method of ~~claim 65~~ <u>claim 63</u> wherein the second authenticating further comprises:

receiving a third message from said unauthenticated client device at said wireless access point, said third message including a third digest, said third digest including a one-way hash function operating on said second random number, said device identifier, and said first secret;

determining a fourth digest at said wireless access point, said fourth digest comprising said second random number, said device identifier, and said first secret;

comparing said third digest to said fourth digest at said unauthenticated client device; and

provided said third digest matches said fourth digest, authenticating said client device to said wireless access point to produce the authenticated client device.

67. (currently amended) The method of ~~claim 65~~ claim 63, further comprising:

determining a fifth digest at said wireless access point, said fifth digest comprising said device identifier received from said authenticated client device, said first secret, said first random number, and said second random number, said fifth digest from which said wireless access point selects bits and determines said key; and

calculating a sixth digest at said client device, said sixth digest comprising said device identifier, said first secret, said first random number and said second random number, said sixth digest from which said authenticated client device selects bits and determines said key.

68. (cancelled)

69. (currently amended) A computer-useable medium having computer-readable code embodied thereon that is executed by a computer to implement ~~the method~~ a method of authenticating an unauthenticated client device and a network access point, said method comprising:

first authenticating a wireless access point to an unauthenticated client device communicatively coupled to the wireless access point via a wireless connection;

second authenticating the unauthenticated client device to the wireless access point to produce an authenticated client device and a key;

third authenticating, via the wireless access point, a user of the authenticated client device to a central authentication server using the key; and

wherein the method of authenticating an unauthenticated client

4

device and a network access point further comprises:

receiving a first message from said unauthenticated client device at said wireless access point, said first message including a device identifier and a first random number;

receiving a second message from said wireless access point at said unauthenticated client device, said second message including a second random number and a first digest, said first digest including a one-way hash function operating on said first random number, said device identifier, and a first secret shared between said wireless access point and said unauthenticated client device;

determining a second digest at said unauthenticated client device, said second digest comprising a one-way hash function operating on said first random number, said device identifier, and said first secret;

comparing said first digest to said second digest at said unauthenticated client device; and

provided said first digest matches said second digest, authenticating said wireless access point to said unauthenticated client device.

70. (cancelled)

71. (currently amended) The computer-useable medium recited in claim 70 claim 69, wherein the method of authenticating an unauthenticated client device and a network access point further comprises:

receiving a third message from said unauthenticated client device at said wireless access point, said third message including a third digest, said

third digest including a one-way hash function operating on said second random number, said device identifier, and said first secret;

determining a fourth digest at said wireless access point, said fourth digest comprising said second random number, said device identifier, and said first secret;

comparing said third digest to said fourth digest at said unauthenticated client device; and

provided said third digest matches said fourth digest, authenticating said client device to said wireless access point to produce the authenticated client device.

72. (previously presented) The computer-useable medium recited in claim 71, wherein the method of authenticating an unauthenticated client device and a network access point further comprises:

determining a fifth digest at said wireless access point, said fifth digest comprising said device identifier received from said authenticated client device, said first secret, said first random number, and said second random number, said fifth digest from which said wireless access point selects bits and determines said key; and

calculating a sixth digest at said client device, said sixth digest comprising said device identifier, said first secret, said first random number and said second random number, said sixth digest from which said authenticated client device selects bits and determines said key.

73. (cancelled)